CLAIMS

The claims are presented for the Examiner's convenience.

1. (Previously Presented) A secure data processing device, the device configured as a Trusted Platform Module (TPM) and comprising:

a secure function module configured to receive an excluding computing module context that enables the secure function module to transact secure functions with an excluding computing module comprising storing cryptographic keys for the excluding computer module;

the secure function module further configured to receive a non-conforming computing module context that enables the secure function module to transact secure functions with a non-conforming computing module comprising storing cryptographic keys for the non-conforming computing module wherein the non-conforming computing module cannot transact the secure function with the secure function module using cryptographic keys of the excluding computing module;

a communication module configured to communicate with the excluding computing module, the excluding computing module configured to exclusively transact the secure function with the secure function module so that the non-conforming computing module must transact the secure function through the excluding computing module, the communication module further configured to communicate with the non-conforming computing module, the non-conforming computing module configured to transact the secure function with the secure function module and unable to transact the secure function through the excluding computing module; and

a context module configured to identify the excluding computing module initiating the secure function and set the context of the secure function module to the excluding computing module context and to identify the non-conforming

computing module initiating the secure function and set the context of the secure function module to the non-conforming computing module context.

2. (Canceled)

3. (Canceled)

4. (Previously Presented) The device of claim 1, wherein context module is configured to arbitrate the setting of the context of the secure function module to either the excluding computing module context or to the non-conforming computing module context.

5. (Original) The device of claim 1, wherein the context module is configured to set the context of the secure function module responsive to an electrical signal.

6. (Previously Presented) The device of claim 5, wherein the electrical signal is an address.

7. (Original) The device of claim 1, wherein the context module is configured to set the context of the secure function module responsive to data communicated to the communication module.

8. (Previously Presented) A computing module, the module comprising:

an identification module configured to identify an excluding computing module to a TPM and set the context of the TPM to an excluding computing module context enabling the TPM to transact a first secure function with the

excluding computing module, the first secure function comprising storing cryptographic keys for the excluding computing module and the excluding computing module configured to exclusively transact the first secure function with the TPM so that a non-conforming computing module must transact the secure function through the excluding computing module;

the identification module further configured to identify the non-conforming computing module to the TPM and set the context of the TPM to a non-conforming computing module context enabling the TPM to transact a second secure function with the non-conforming computing module wherein the non-conforming computing module cannot transact the secure function with the TPM using cryptographic keys of the excluding computing module, the second secure function comprising storing cryptographic keys for the non-conforming computing module;

an address module configured to address a secure function of the TPM; and

a data module configured to exchange data with the TPM.

9. (Previously Presented) The module of claim 8, the identification module further configured to identify the excluding computing module and non-conforming computing module with an address communicated from the address module.

10. (Previously Presented) The module of claim 8, the identification module further configured to identify the excluding computing module and non-conforming computing module with data communicated from the data module.

11. (Previously Presented) A secure data processing system, the system comprising:

a TPM configured to identify a computing module responsive to the computing module initiating transacting a secure function with the TPM, the TPM further configured to set the context of the TPM to the computing module context enabling the TPM to transact the secure function with the computing module, wherein the TPM is configured to transact the secure function with the computing module, the secure function comprising storing cryptographic keys for the computing module;

an excluding computing module configured to initiate transacting the secure function with the TPM, the excluding computing module further configured to exclusively transact the secure function with the TPM so that a non-conforming computing module must transact the secure function through the excluding computing module; and

the non-conforming computing module configured to initiate transacting the secure function with the TPM, the non-conforming computer module further configured to transact the secure function with the TPM wherein the non-conforming computing module cannot transact the secure function with the TPM using cryptographic keys of the excluding computing module.

12. (Canceled)

13. (Canceled)

14. (Previously Presented) The system of claim 11, wherein the TPM identifies the excluding computing module and non-conforming computing module from an electrical signal.

15. (Original) The system of claim 14, wherein the electrical signal is an address.

16. (Previously Presented) The system of claim 11, wherein the TPM identifies the excluding computing module and non-conforming computing module from a data value.

17. (Previously Presented) A computer readable storage medium comprising computer readable code executable by a digital processing apparatus, the computer readable code configured to:

identify a computing module as an excluding computing module if the computing module is an excluding computing module, the excluding computing module configured to exclusively transact a secure function with a TPM so that a non-conforming computing module must transact the secure function through the excluding computing module;

identify the computing module as the non-conforming computing module if the computing module is a non-conforming computing module, wherein the non-conforming computing module cannot transact the secure function with the TPM using cryptographic keys of the excluding computing module;

set the TPM to an excluding computing module context if the computing module is the excluding computing module enabling the TPM to transact the secure function with the excluding computing module and a non-conforming computing module context if the computing module is the non-conforming computing module enabling the TPM to transact the secure function with the non-conforming computing module; and

transact the secure function comprising storing cryptographic keys

between the TPM and the computing module, wherein the transaction is restricted to a secure function and sensitive data of the computing module context.

18. (Canceled)

19. (Previously Presented) The computer readable storage medium of claim 17, further comprising computer readable code configured to identify the excluding computing module and non-conforming computing module as an initiator of the secure function transaction.

20. (Previously Presented) The computer readable storage medium of claim 17, further comprising computer readable code configured to arbitrate the setting of the context of the TPM between the excluding computing module and the non-conforming computing module.

21. (Previously Presented) The computer readable storage medium of claim 17, further comprising computer readable code configured to identify the excluding computing module and non-conforming computing module responsive to an electrical signal.

22. (Previously Presented) The computer readable storage medium of claim 17, further comprising computer readable code configured to identify the excluding computing module and non-conforming computing module responsive to an address.

23. (Previously Presented) The computer readable storage medium of claim 17, further comprising computer readable code configured to identify the excluding computing module and non-conforming computing module responsive to a data value.

24. (Previously Presented) A secure computing method, the method comprising:

identifying a computing module as an excluding computing module if the computing module is an excluding computing module, the excluding computing module configured to exclusively transact a secure function with a TPM so that a non-conforming computing module must transact the secure function through the excluding computing module;

identifying the computing module as the non-conforming computing module if the computing module is a non-conforming computing module;

identifying the computing module as the non-conforming computing module if the computing module is the non-computing module, wherein the non-conforming computing module cannot transact the secure function with the TPM using cryptographic keys of the excluding computing module;

setting a TPM to an excluding computing module context enabling the TPM to transact a secure function with the excluding computing module if the computing module is the excluding computing module and a non-conforming computing module context enabling the TPM to transact the secure function with the non-conforming computing module if the computing module is the non-conforming computing module; and

transacting the secure function comprising storing cryptographic keys between the TPM and the computing module, wherein the transaction is restricted to a secure function and sensitive data of the computing module context.

25. (Canceled)

26. (Original) The method of claim 24, further comprising initiating the transacting of the secure function.

27. (Previously Presented) The method of claim 24, further comprising arbitrating the setting of the TPM context between the excluding computing module and the non-conforming computing module.

28. (Previously Presented) The method of claim 24, wherein an electrical signal identifies the excluding computing module and the non-conforming computing module.

29. (Previously Presented) The method of claim 24, wherein a data value identifies the excluding computing module and the non-conforming computing module.

30. (Previously Presented) An apparatus for secure computing, the apparatus comprising:

means for identifying a computing module as an excluding computing module if the computing module is the excluding computing module, the excluding computing module configured to exclusively transact a secure function with a TPM so that a non-conforming computing module must transact the secure function through the excluding computing module;

means for identifying the computing module as the non-conforming computing module if the computing module is the non-conforming computing module, wherein the non-conforming computing module cannot transact the secure function with the TPM using cryptographic keys of the excluding computing module;

means for setting the TPM to an excluding computing module context

enabling the TPM to transact a secure function with the excluding computing module if the computing module is the excluding computing module and a non-conforming computing module context enabling the TPM to transact the secure function with the non-conforming computing module if the computing module is the non-conforming computing module; and

means for transacting the secure function comprising storing cryptographic keys between the TPM and the computing module, wherein the transaction is restricted to a secure function and sensitive data of the computing module context.